Method and System for Maintaining Network Activity Data for Intrusion Detection
Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
Sheet: 1 of 4 Filed: December 20, 2000

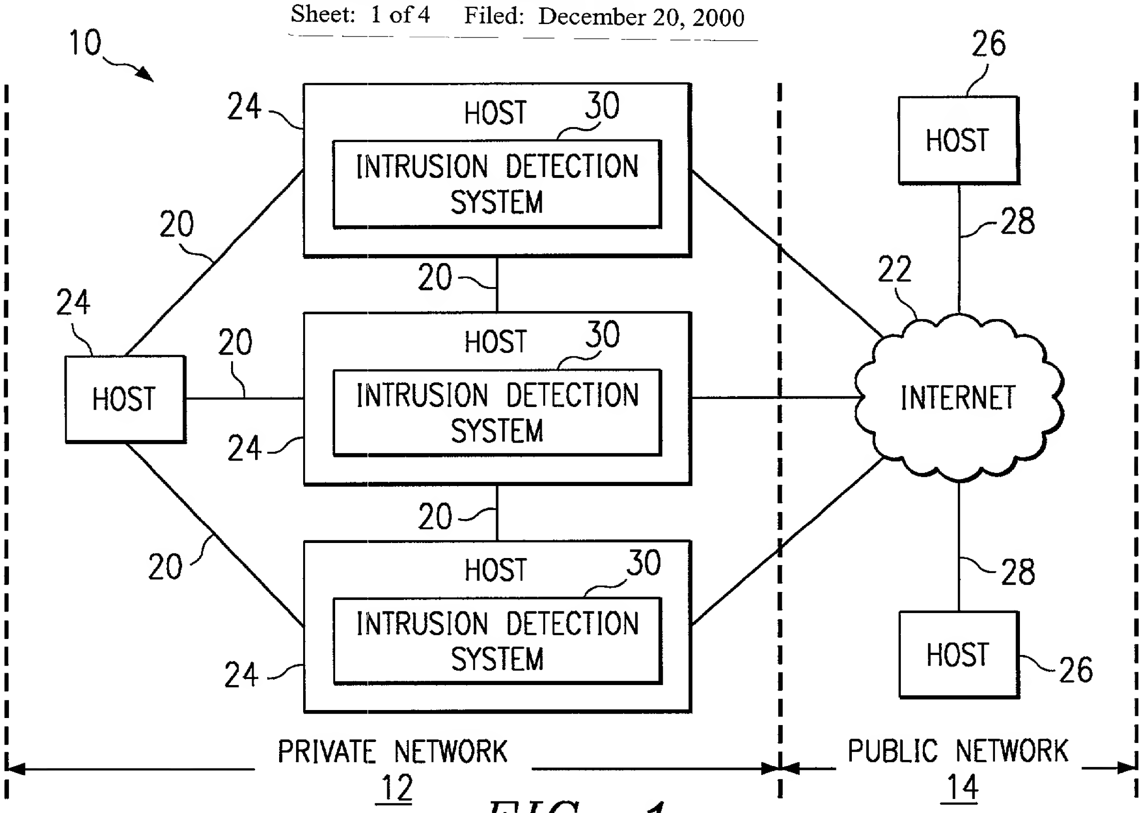

FIG. 1

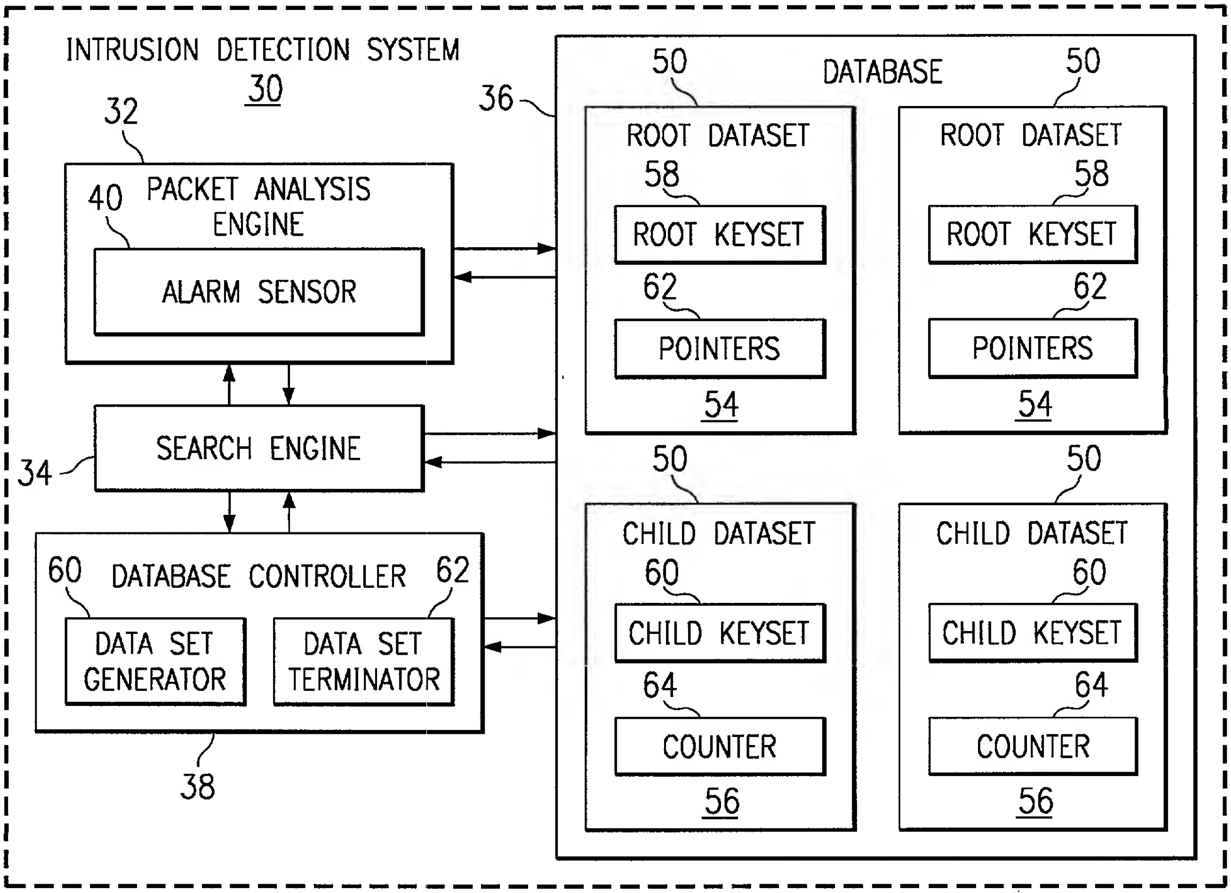

FIG. 2

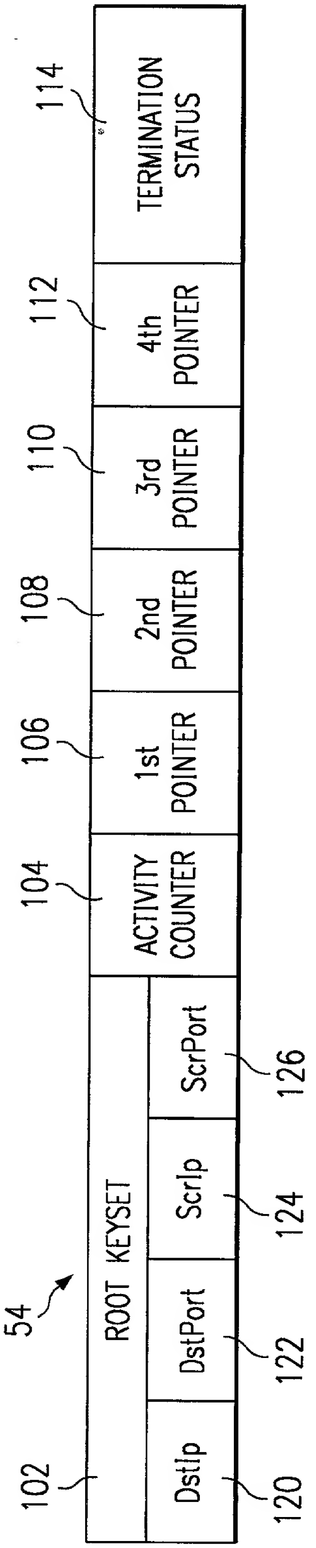

FIG. 3A

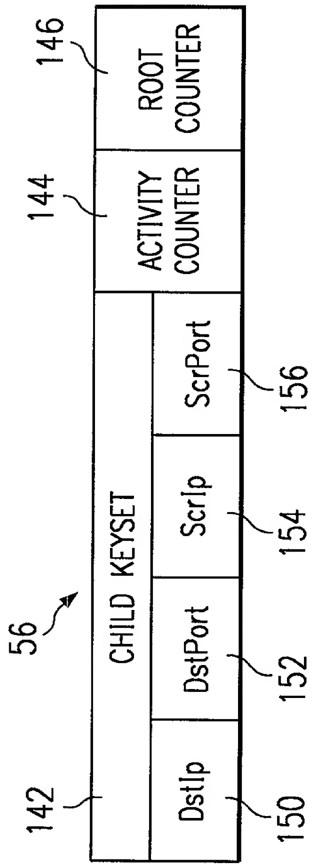

FIG. 3B

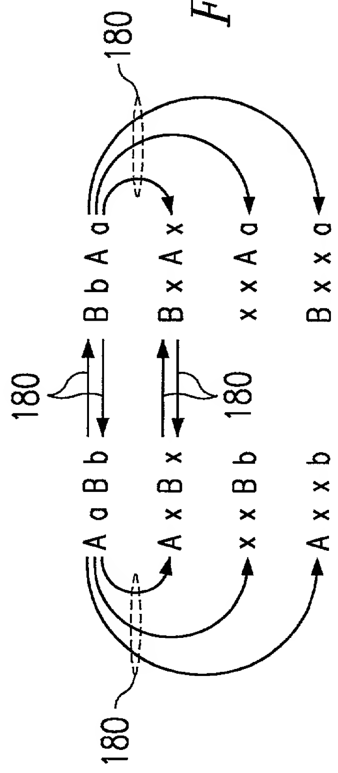

FIG. 4

Method and System for Maintaining Network Activity Data for Intrusion Detection
Inventor: Wiley, et al.
Attorney's Docket: 062891.0424
Sheet: 3 of 4 Filed: December 20, 2000

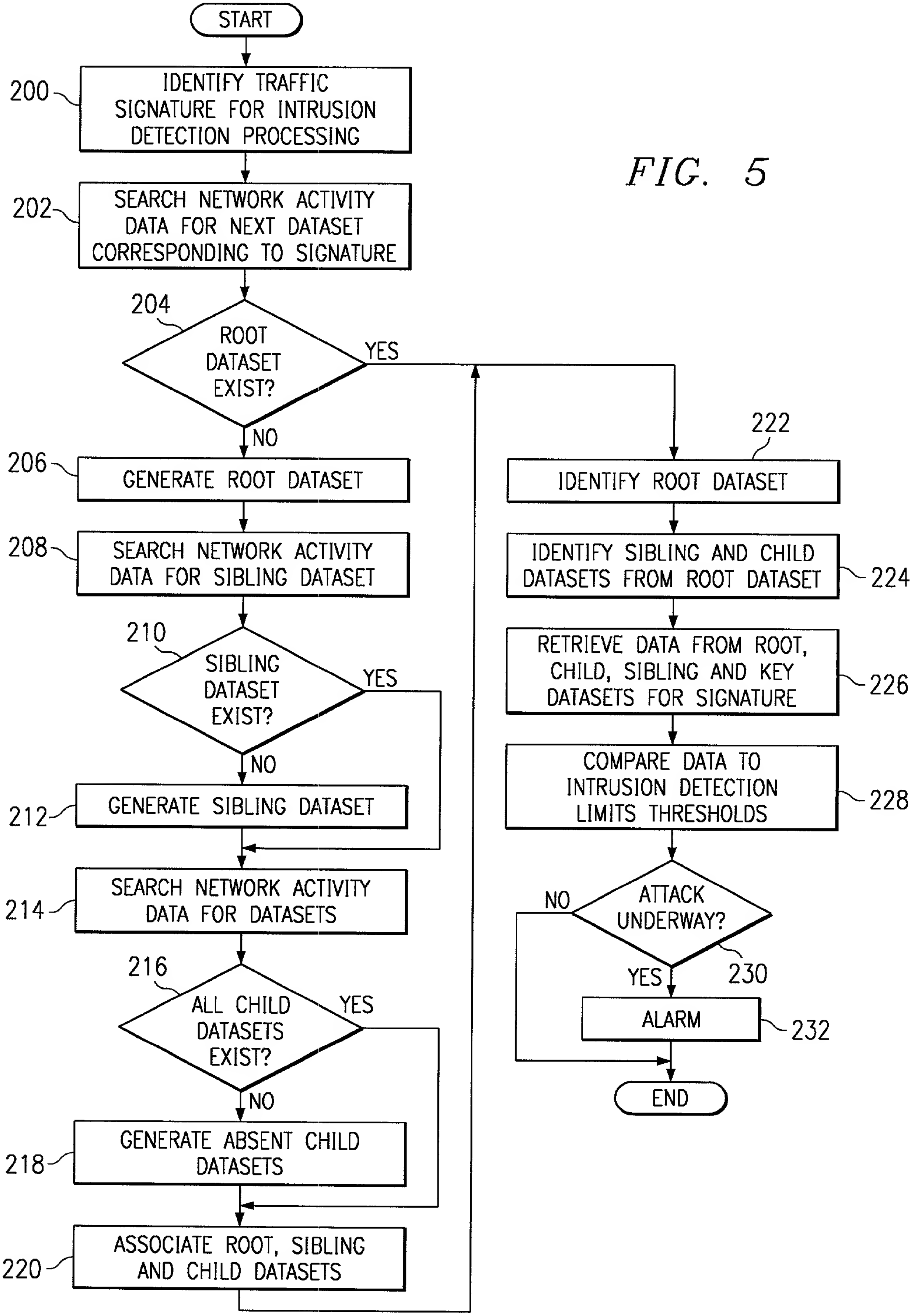
START
200
IDENTIFY TRAFFIC SIGNATURE FOR INTRUSION DETECTION PROCESSING
202
SEARCH NETWORK ACTIVITY DATA FOR NEXT DATASET CORRESPONDING TO SIGNATURE
204
ROOT DATASET EXIST?
YES
NO
206
GENERATE ROOT DATASET
208
SEARCH NETWORK ACTIVITY DATA FOR SIBLING DATASET
210
SIBLING DATASET EXIST?
YES
NO
212
GENERATE SIBLING DATASET
214
SEARCH NETWORK ACTIVITY DATA FOR DATASETS
216
ALL CHILD DATASETS EXIST?
YES
NO
218
GENERATE ABSENT CHILD DATASETS
220
ASSOCIATE ROOT, SIBLING AND CHILD DATASETS
222
IDENTIFY ROOT DATASET
224
IDENTIFY SIBLING AND CHILD DATASETS FROM ROOT DATASET
226
RETRIEVE DATA FROM ROOT, CHILD, SIBLING AND KEY DATASETS FOR SIGNATURE
228
COMPARE DATA TO INTRUSION DETECTION LIMITS THRESHOLDS
230
ATTACK UNDERWAY?
NO
YES
232
ALARM
END

FIG. 5

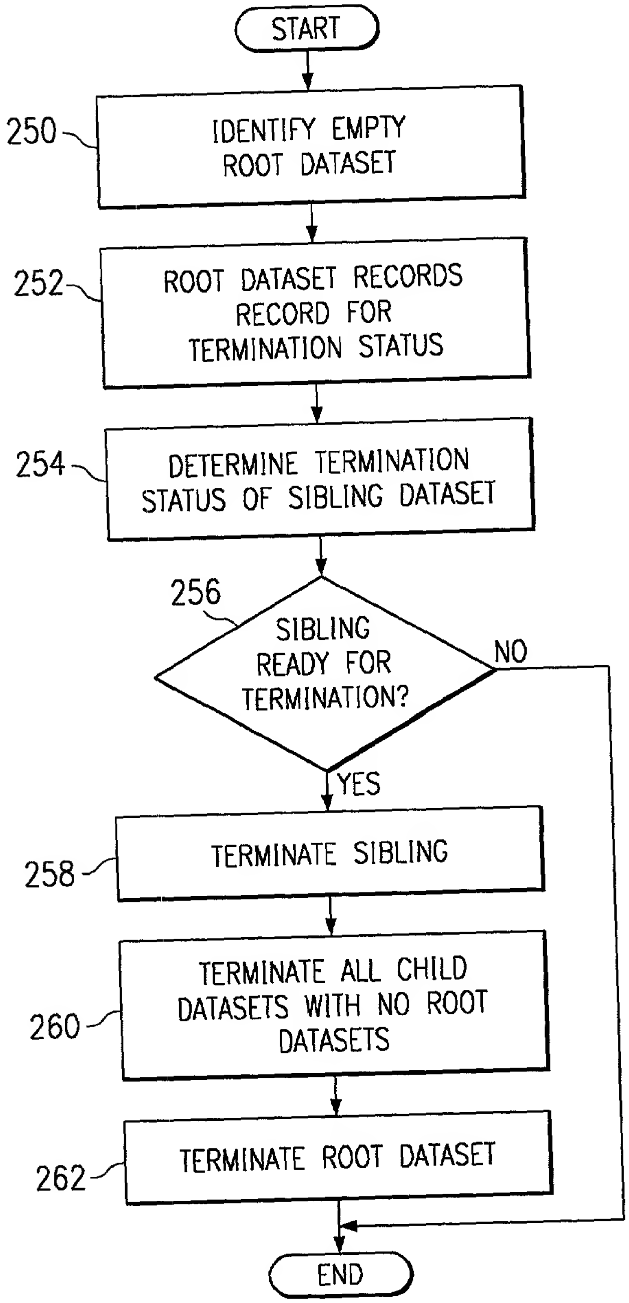
START
250
IDENTIFY EMPTY ROOT DATASET
252
ROOT DATASET RECORDS RECORD FOR TERMINATION STATUS
254
DETERMINE TERMINATION STATUS OF SIBLING DATASET
256
SIBLING READY FOR TERMINATION?
NO
YES
258
TERMINATE SIBLING
260
TERMINATE ALL CHILD DATASETS WITH NO ROOT DATASETS
262
TERMINATE ROOT DATASET
END

FIG. 6